Distributed Access Control on IoT Ledger-based Architecture

Roben Castagna Lunardi*†, Regio Antonio Michelin*†, Charles Varlei Neu*‡ Avelino Francisco Zorzo*
*PUCRS, †IFRS,‡UNISC - Brazil
E-mail: {roben.lunardi, regio.michelin, charles.neu}@acad.pucrs.br, avelino.zorzo@pucrs.br

***Abstract*—Due to increased number of attacks on the Internet of Things (IoT) devices, the security of IoT networks became critical. Some recent researches proposed the adoption of blockchain in IoT networks without a thorough discussion on the impact of the solution on the devices performance. Furthermore, blockchain employment in the context of IoT can be challenging due to the devices hardware limitations. To fill this gap, this paper proposes an IoT ledger-based architecture to ensure access control on heterogeneous scenarios. This research applies conventional devices used on IoT networks, such as Arduino, Raspberry and Orange Pi boards. Finally, we perform performance evaluation focused on access control of IoT devices and on information propagation through peers on a private IoT network scenario.**

I. Introduction

Access management has been investigated by many researchers in the past decades. Despite of that, many security issues are still open and, therefore, problems on access management could compromise not only a single device/system/network, but also different services on the Internet. On October, 2016 a famous attack against a service had a huge impact on many other services on the Internet. Particularly in that attack, the Mirai botnet [1] used devices with default configurations (specially default user and password) to attack a dynamic Domain Name Server (DNS) provider, *i.e.* the Dyn DNS. In that attack, millions of devices, *e.g.* IP cameras, vacuum cleaners, and domestic routers, were used to produce a Distributed Denial of Service (DDoS) attack. Consequently, different applications and services that were using this dynamic DNS provider became unavailable [1]. This single example shows the importance of access management in a context in which several different devices ("things") are connected to the Internet, *i.e.* the Internet of Things.

Over the years many authors proposed different meanings for the term "Internet of Things" (IoT) [2] [3] [4]. In this paper, we consider IoT as an environment composed of smart objects with different hardware capabilities connected through a TCP/IP network. Many IoT networks are composed by devices with different hardware constraints, limited processing power, low energy consumption and specific communication protocols. Furthermore, some aspects of an IoT environment can be challenging when trying to apply a unified solution for access management: (*i*) **decentralization** - devices should collaborate to process the produced information and the authentication method should not be centralized; (*ii*) **resilience** - system/application should work even if a device is down or not available; (*iii*) **tamper-resistance** - data transmitted by sensors should not be modified, nor the author of the information should be changed; and (*iv*) **lightweight solution** - mechanisms adopted both to transfer information and to ensure a secure connection should be adequate to the hardware constraints.

978-1-5386-3416-5/18/$31.00

In the context of a decentralized, resilient and tamper-resistant alternatives, Bitcoin introduced the concept of blockchain as a novel solution for cryptocurrency [5]. In that solution, information integrity is guaranteed by the signature of the peer that produced the information. Also, every peer can verify any transaction using the public key of the peer that performed a transaction (and wrote the information into the chain). As a consequence, blockchain contains every transaction performed over the time and therefore it is not a lightweight solution. In other words, a blockchain can be defined as a distributed and decentralized ledger that contains connected blocks of transactions. Many other alternative blockchain implementations were proposed in recent years, such as Ethereum, Namecoin and Hyperledger [6].

Naturally, after the proposal of different implementations of blockchain, some questions on its use in IoT networks need to be answered, *e.g.*: 1) How IoT devices can handle cryptography algorithms used in a blockchain?; 2) How blockchain could be adapted to support Access Management on IoT networks?; 3) What is the impact of blockchain on constrained devices?

In order to help answering the first question, this paper presents a discussion regarding characteristics of current blockchain implementations that can be used in an IoT environment. Regarding the second question, some aspects were considered in this paper, for example, which kind of devices will be used in an IoT network, considering their hardware capabilities; how the devices will be accessed; and, some of the security concerns for the adopted access control method. Moreover, we propose an IoT ledger-based architecture, which was implemented through a chain based on the hash of block headers and block ledger (composed by a ledger of signed information) for each device. Finally, to answer the last question, we performed some experiments to evaluate the behaviour of constrained devices handling an IoT ledger-based architecture. This work intends to explore these aspects, bring some answers, and evaluate the proposed IoT ledger.

II. Related Work

In the last few years, different solutions were proposed in the context of IoT networks. For example, some researches focused on communication and management protocols [7], on distributed dissemination and processing of information [8], or on access control, specially on authentication and authorization, confidentiality, integrity and tamper-resistance [4] [9] [10]. Although the solutions proposed by previous researchers presented some improvements to IoT networks, some open issues related to IoT security remain, for example, (*i*) use of existent protocols and services, or standardization of new ones, for security in IoT scenarios, specially for authentication; and, (*ii*) definition of architectures and models to ensure resilience and confidentiality through a heterogeneous environment.

The adoption of blockchain technology could be a challenge for IoT networks [11]. The main problem regarding the use of blockchain in IoT is related to the hardware capabilities of the devices that run on the IoT context. This limitation requires lightweight solutions, and most of the public blockchain size makes them inapplicable for IoT. Another problem regarding hardware limitation is related to computing power of IoT devices. For example, Bitcoin [5] applies the Proof-o-Work (PoW) consensus algorithm, which uses hash brute force calculation and, therefore, demands a lot of time, processing power and energy to achieve consensus.

One evaluation of consensus algorithms is presented in Christidis [12] research. This research investigated different consensus algorithms such as Sieve, Practical Byzantine Fault Tolerant, Proof-of-Stake and Proof-of-Work. As indicated in that work, the mechanism used in blockchains depends on two factors: the network in which it will be used and the attack vector that is intended to be mitigated. Consequently, the number of nodes and the processing overhead are important issues to be considered. Despite the application examples evaluated in Christidis' research, none of them applied blockchain as an identity manager or authentication service.

Huh *et al.* [13] proposed a scenario using Ethereum and smart contracts to manage an IoT environment. After some experiments, some problems of running Ethereum on Raspberry Pi boards were discussed. The two major weakness of using Ethereum for IoT were: the time spent to update the blockchain (problem related to the consensus algorithm) and the requirement of a large storage size.

Ouaddah [9] research presented an evaluation considering the application of different access control mechanisms to the IoT context. The research considered criteria such as device heterogeneity, scalability and lightweight in order to identify the best solution for the IoT domain. The paper indicated as future direction the blockchain application in the IoT architecture to handle access management. Thus, proposing a lightweight consensus algorithm and blockchain storage strategy are crucial in order to apply the blockchain solution to the IoT context.

Dorri *et al.* [14] proposed a lightweight blockchain architecture for IoT as an authorization mechanism to access data in Smart Homes. Basically, the devices with limited hardware are more susceptible to attacks, specially to: *Denial of Service* (*DoS*), *Modification Attack*, *Dropping Attack*, and *Appending Attack*. In order to mitigate these problems, the use of overlays was proposed. In that environment, computers are used to maintain a blockchain with information of the devices. Although simulations point to a reduction on devices' processing overhead and on the number of packets on the network, it did not discuss how the devices are authenticated nor how limited power devices could be used in the environment.

Boudguiga *et al.* [15] research was focused on the employment of blockchain to ensure updated information about IoT devices data and availability. The paper also presents some questions about different scenarios in which IoT is used, such as Smart Homes, Smart Grids, Industry 4.0, and Intelligent Transportation Systems. In order to cover these scenarios, the research proposed the use of two distinct infrastructures: one for blockchain devices in a MultiChain architecture (Blockchain-as-a-Service) and another for IoT devices. Nevertheless, there was no experimental evaluation of the proposed solution.

Furthermore, some papers discuss security in different layers of an IoT context [16] [17] [18]. Jing [19], *e.g.*, proposed a three-layer architecture (Perception, Transportation and Application) and discussed security issues and challenges in each layer. Nonetheless, a solution that considers hardware restriction in each layer was not presented.

The use of blockchain has been a prominent solution to solve security issues on IoT networks, as indicated by the previously mentioned related work. However, they did not consider the access management in IoT Networks composed by devices with different capabilities. Moreover, few researchers evaluate the performance to use cryptography and blockchain in a single architecture. In the next sections, we fill this gap by presenting an architecture for IoT networks that uses blockchain to help the Distributed Access Control of devices, as well as, we evaluate the proposed solution through heterogeneous devices.

III. IoT Ledger-based Architecture

Many authentication solutions proposed for IoT use different encryption algorithms through the communication layer. Despite that, to the best of our knowledge, none tackles one of the major problems in IoT networks, *i.e.* the use of devices with different hardware specification. Therefore, a new authentication mechanism has to ensure that it could provide enough security despite the capacity of the device running it. In order to guide the design of our proposed solution, the Kill Chain attack model [20] was considered. In this attack model, 7 different chained steps should be performed by attackers to get their objective. Hence, if attackers achieve the seventh step, they cannot be able to affect the integrity of information from other devices (*e.g.*, producing a tampered information about other devices) nor compromise system availability (*e.g.*, a DDoS attack should not affect the whole network).

Based on current architecture solutions for security in IoT environments, which consider a set of features that should be provided [21], *e.g.* multilayer, hardware limitation, gateway usage, etc., this paper proposes a multilayer architecture in which (*i*) *perception layer* represents devices, such as sensor and actuators; (*ii*) *transportation layer* is responsible for managing IoT gateways; and (*iii*) *application layer* represents external services and user applications. Figure 1 shows the proposed architecture. This architecture considers IoT devices heterogeneity, and these devices are organized in multiple layers. Basically, the architecture contains devices and gateways.

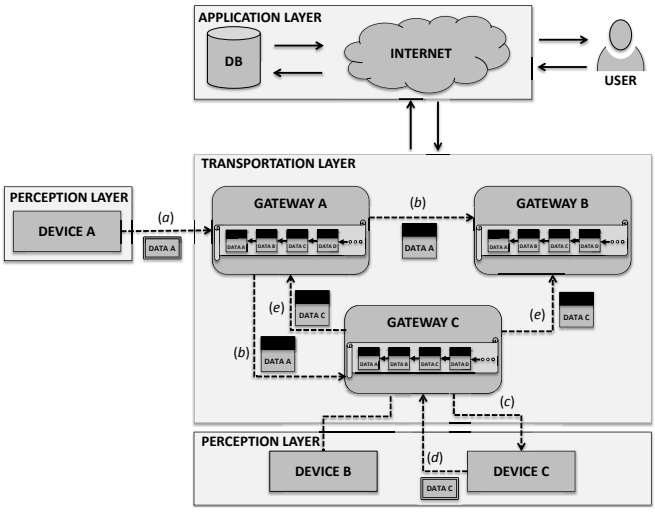

Fig. 1. Proposed IoT ledger-based architecture

Gateways are places in which our proposed blockchain (also referred in this paper as the IoT ledger) will be processed and stored. The components of the proposed architecture are:

- *Devices*: equipment, such as sensor or actuator, that are responsible to send data to (temperature, humidity, movement sensors) or receive commandos from (buzzer, relays, motors) the gateway. The *Perception Layer* is responsible for a full-duplex communication between devices and gateways. Each device is responsible for providing/receiving information. In the proposed architecture, it is assumed that each device has a key pair generated priory and embedded in its own firmware, thereby, a public key can be sent to all gateways, while the private key is kept secret and used to encrypt and sign information. Hence, once information is sent to a gateway, this information is encrypted using the device private key.
- *Gateway*: Gateways in IoT plays the role of interconnecting heterogeneous devices, as it translates information to the same protocol that is used by devices. Also, it stores the data collected from devices. In the proposed architecture, a gateway is also responsible to maintain an IoT ledger copy. Once information is received by the gateway, it is responsible to validate and sign the information using its own private key. This signed data is appended to the corresponding device block in the IoT ledger and sent to its peers.
- *Transportation Layer*: *Transportation Layer* is represented through the interconnection of gateways. This interconnection is executed creating a P2P network in which each gateway represents a peer. Over this P2P network, blocks are exchanged between gateways in order to keep the IoT ledger updated.
- *IoT ledger*: The gateway is responsible for keeping the IoT ledger. For the proposed architecture, each block is composed of a header and content. The block header is used to create the chain, since the header hash value of the previous block is added to the next header block. The block ledger is composed by the device produced information. Thus each block is bound to a specific device, and its information is kept in the content inside a block. The access to that information is provided through the *application layer*.

In a regular operation, through the proposed architecture, a device is responsible for producing information. This information is signed by the device and sent to the gateway (as can be observed in step (*a*) in Figure 1). Once the information is received by the gateway, it is responsible for double signing the information in order to keep track of which gateway was responsible for inserting/appending information in a block inside the IoT ledger. As soon as the information is double signed, it is sent to the connected peers with the purpose of keeping all IoT ledger copy updated (*b*). Likewise, when an information is sent to a device (*c*), for example to activate a relay switch circuit, it is signed again by the device (*d*), double signed by the gateway and publicized to peers (*e*).

As a blockchain proposal for our architecture, each device is mapped to a block in an IoT ledger. Consequently, the IoT ledger will contain as many blocks as devices connected to the network. Through this approach, the devices are able to move along the IoT gateways with no further action required. It will also ensure the network resilience, since each gateway has an IoT ledger copy.

The gateways are devices with limited storage and processing power. Thus, for each gateway, it will be possible to parameterize and define the amount of information that is stored in the local IoT ledger. So, once the limit has been reached, the new information produced is maintained in the block ledger, and the older content can be uploaded and appended to an external storage in the *application layer*. This external storage can also be represented by an external ledger and preserved in a cloud environment. It is important to notice that this feature is not in the scope of this work.

Before any device performs its first transaction in the IoT, it should authenticate through a gateway. For example, in Figure 1, Device A is authenticated in the IoT ledger through Gateway A. After that, the device has to perform a Key Exchange procedure with the gateway to build a secure channel. This procedure is presented as follows:

1) Device A sends a Hello message with its own Public Key (*e.g.*, for encryption using the RSA algorithm) to

Gateway A;

2) Gateway A sends a randomly generated symmetric key (*e.g.*, to build an AES secure channel) encrypted with the device's Public Key;
3) Device A starts sending data through an encrypted channel using the AES key generated by the gateway.

The device identification scheme is based on the public and private key pair. While the device private key should be kept secret, the public key (represented as DevicePubKey in Figure 2) will be publicized and used by the gateway to identify the device. The device provided *Data* and *Time* (timestamp from the time in which information was generated) will be signed using its private key (represented as *SD*) and stored in a block as shown in Figure 2. The information (*Data*) will be double signed by the gateway (represented as *SGw*), which will append the information from the device in the *Block Ledger* (a chain of signed data from the same device). Also, the gateway will append the previous hash (represented as *HashPrev*), *i.e.*, hash of the previous block in the *Block Ledger*, to ensure that no information will be lost.

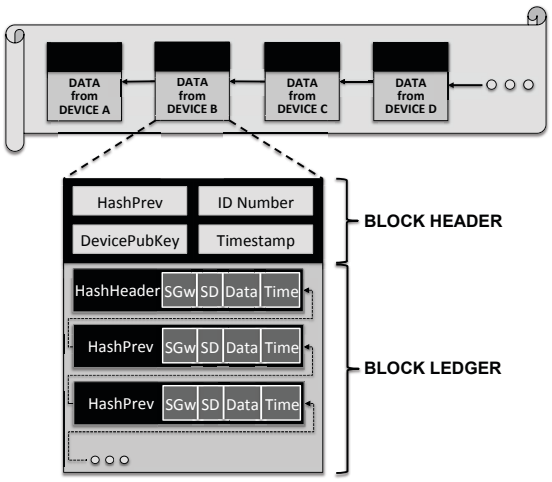

Fig. 2. Block structure

It is important to mention that the first "Previous Hash" on each *Block Ledger* will be the hash of the *Block Header* (called *HashHeader* in Figure 2). Different from the Bitcoin blockchain, which has a characteristic that the block contains a set of transactions and the block is immutable [5], in our proposal, only the block header is immutable while the block payload information can be appended. Thus the *Block Header* stores the *previous block header hash* (based on this data the chain is created); a block *ID Number*, which is a sequential unique block identifier; the *Device Public Key*, which is used to perform any communication from/to devices connected to the IoT architecture; and a *timestamp*, which keeps track of the time when the block was created in the IoT ledger.

A. Resilient and Robust Access Control - R2AC

Based on the conceptual IoT ledger-based architecture, presented previously, we built a prototype system called Resilient and Robust Access Control (R2AC). The R2AC aims to help heterogeneous devices (*e.g.*, different processing capabilities and energy requirements) to exchange information regarding state of sensors and actuators. Also, R2AC allows registered devices to connect to any gateway of the IoT network, performing a distributed and resilient access control. Finally, R2AC implements the IoT ledger presented in Figure 1. This implementation was initially designed to be used in different scenarios, such as Smart Buildings and Smart Cities.

R2AC consists of a P2P communication, REST architecture over HTTP, an authentication method (based on predefined public key for each device), and a lightweight blockchain implementation. Hence, our proposed IoT ledger was improved to reflect the chain proposed in the conceptual architecture, specially the proposed block ledgers presented in Figure 2.

As a proof of concept, the prototype implementation used in the scope of this paper does not consider an specific consensus algorithm. This decision was made considering a small scenario of only three gateways in a controlled environment. Thus, for the evaluation of our proposed IoT ledger, it was considered that every block is trusted since the Block Hash is correct. Also, the communication with an external cloud database was not considered. This communication is necessary to store/retrieve information about old data from devices nor the (web) interface to access the information from gateway. Both consensus algorithm and retrieval database and information mechanisms will be discussed in a future work. Consequently, the experimental evaluation (presented in Section IV) is focused on the secure connection from devices to gateways and on the capabilities of gateways to handle the insertion of information in the proposed IoT ledger.

IV. Experimental Evaluation

An important aspect to implement a blockchain in an IoT multi-tier architecture is to verify its applicability on a specific scenario. Furthermore, it is crucial to consider how the most constrained devices can handle the solution. Additionally, the cryptography and hash functions play a crucial role to the blockchain application. Thus, its evaluation could indicate the hardware that fits better the requirements. As examples of constrained devices, Arduino and Raspberry Pi boards are widely used to control devices over the Internet. For this analysis, the following devices were chosen: Arduino UNO, a micro-controller board based on Atmel ATMega 328P (16 MHz clock and 32KB of memory); Raspberry Pi 2 B Boards (900MHz quad-core ARM Cortex-A7 CPU and 1GB of memory); Orange Pi Zero (1.2GHz ARM Cortex-A7 CPU and 256MB of memory); and regular PC (Intel®Core™i3 M350@2.27GHz, 8GB SODIMM DDR3 RAM, 120GB SSD, Linux Ubuntu 14.04), which was chosen to establish performance baseline.

A. Cryptography Performance

First, some experiments were performed with the RSA algorithm - often used for key exchange. It is important to verify how devices can handle this algorithm, since it

is known to be time consuming. After that, an evaluation was performed to understand how these devices can handle the SHA256 algorithm - used on many blockchains, such as Bitcoin, to create block and transaction hashes. After that, we performed an evaluation on how the boards can handle AES symmetric algorithm (less time consuming than RSA), commonly used to build secure communication. Also, some experiments were performed to verify how the boards would handle both cryptography and hash algorithms - for example, to send encrypted data and hash. For both RSA and AES cryptography algorithms, due to hardware constraints, we used predefined fixed keys. The results presented in Table I show the median value for 10 samples with a standard deviation smaller than 0.004ms.

TABLE I
PERFORMANCE OF CONSTRAINED DEVICES (RSA, AES256, SHA256)

	Ard. UNO	**Rasp. Pi 2**	**Orange Pi**	**PC**
RSA Encrypt	15.0ms	0.4ms	0.36ms	0.07ms
RSA Decrypt	9966.1ms	0.5ms	0.5ms	0.1ms
SHA256	22.3ms	0.16ms	0.18ms	0.03ms
RSA+SHA256	63.8ms	1.1ms	0.8ms	0.14ms
AES Encrypt	6.5ms	0.07ms	0.07ms	0.01ms
AES Decrypt	25.9ms	0.06ms	0.07ms	0.01ms
AES + SHA256	32.6ms	0.25ms	0.3ms	0.03ms

Based on the results presented in Table I, we identified that even Arduino, which has limited memory and processing power resources, was able to run the RSA algorithm. However it takes a considerable amount of time to get the text ciphered and deciphered, when compared to Raspberry Pi 2, Orange Pi Zero or PC. For example, text deciphering RSA using Arduino took around 10,000 ms, while the same text deciphering using Raspberry Pi 2 or Orange Pi Zero took only 0.5 ms. This difference becomes smaller when the SHA256 hash algorithm is executed. In that case, the difference reduces to 22 ms. Thus, taking this results into account, Raspberry Pi 2 and Orange Pi Zero were chosen to host the IoT ledger execution (gateway), while Arduino will only be used to manage sensors and actuators.

B. Performance to append a Block

Since Raspberry Pi 2 and Orange Pi Zero play the gateway role in the proposed architecture, their performance was compared to Personal Computer (PC) in order to establish a time parameter of hosting the IoT ledger. Two operations were executed: (*i*) AES key generation, which consists of the operation when a device is beginning a communication to gateways and, at this point, the gateway will generate an AES key and cipher this random key using the device RSA public key fetched from the block header in the IoT ledger; and (*ii*) appending information to an existing device block, where the gateway receives a package containing information and the device signature; after that, the gateway, using its own RSA private key, signs the package and appends it to the block in the block ledger.

The results (evaluated in both situations) had better performance when executed in the PC - at least 5 times faster - than in Raspberry Pi 2 or Orange Pi Zero. However, as the IoT architecture proposed considers the use of constrained hardware, Raspberry Pi and Orange Pi showed acceptable results in terms of processing time.

Analyzing the results from Raspberry Pi 2 and Orange Pi Zero, we noticed that the operation to sign and append new information to a block (structured as shown in Figure 2) is more time consuming than the key generation and encryption using AES. Thus, the time value to append new information into a block in the IoT ledger has an average time of 45.7 ms on Orange Pi Zero and 20.99 ms on Raspberry Pi 2. Also, considering the confidence interval value, it will ensure that 95% of samples range from 45.27 to 46.13ms on Orange Pi Zero and 20.69 to 21.31 ms on Raspberry Pi 2. Moreover, the AES key generation also ensures that 95% of samples range from 2.76 to 2.80 ms on Orange Pi Zero and 3.29 to 3.89 ms on Raspberry Pi 2.

C. Proposed Ledger Evaluation

In order to evaluate the viability to use a Distributed Access Control in an IoT network, we have carried out experiments using **R2AC**. In these experiments, we focused our attention on the performance of gateways and the time spent to append new information through the block ledger and to propagate that to other gateways.

We considered, in this evaluation, a three floor building environment with lighting controlled by smart devices. Each floor is managed by a gateway (*e.g.* Raspberry Pi 2 B or Orange Pi Zero). Also, each room has luminosity sensors, dimmers and relay managed by one or more devices (*e.g.* Arduino boards). Thus, the IoT infrastructure employed in this evaluation is composed by 3 gateways - one Raspberry Pi 2 and two Orange Pi Zero, all of them with Raspbian OS - and devices (Arduino UNO) to measure and control the lightning.

In this scenario, we assumed that each device was registered previously by an administrator. Consequently, each Block Header (with the device public key) in the IoT ledger was already created when the experiments started. After the key exchange procedure (to use an AES Key generated by the gateway), a device sends 100 data updates, in a rate of one update per second, to the corresponding gateway. Each update is appended to the corresponding block in the IoT ledger and propagated to the other gateways. The experiment was repeated 10 times and we present the median time for each block in sequence.

Figure 3 presents the median time to append the data received from the device to generate both gateway signature and hash of the previous block, append it to the IoT ledger and send it to other peers. As can be observed in Figure 3, gateway *Gw A* takes from 45 to 70 ms to append and send the block generated to the other gateways.

Additionally, the time to append a block (to the block ledger) into gateways *Gw B* and *Gw C* was measured (gateways that are not directly connected to the device that sends information). It is important to mention that only the time spent after the other gateways received the block is considered,

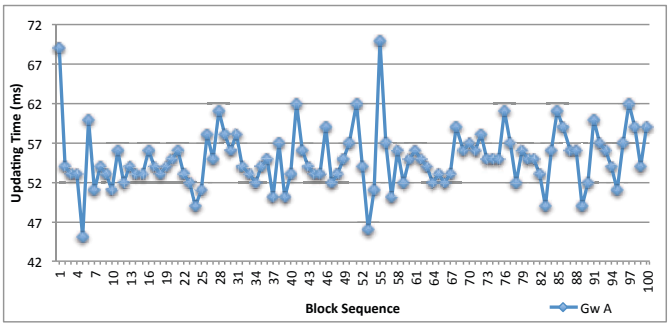

Fig. 3. Performance for appending and sending information to the gateways

i.e., the time spent to send a block onto the network is not considered. As can be observed in Figure 4, the time to append a block on *Gw B* goes from 0.4 to 0.8 ms and on *Gw C* from 0.4 to 0.83ms.

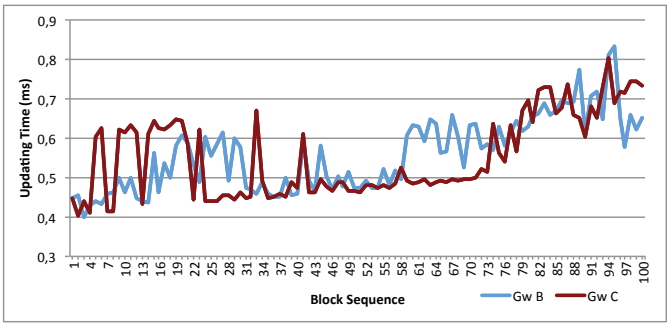

Fig. 4. Performance for appending new information on Block Ledger

Considering the evaluated scenario, *Gw A* (gateway that controlled the device) takes around 5 to 7% of time between updates to generate a block, to append it to the IoT ledger and to send it to other gateways. Furthermore, *Gw B* and *Gw C* take less than 0.1% of time between updates to append information into the block ledger. Consequently, the proposed IoT ledger presented promising performance results. However, it is important to evaluate the solution with a higher number of devices and gateways.

D. Discussion

The main goal of these experiments was to identify the device's capability to access an IoT ledger through encrypted communication channels. Firstly, the experiments helped to identify what component could be used to play the gateway role in an IoT network. As can be observed in Table I, Orange and Raspberry Pi performed much better than Arduino and had acceptable results as an IoT gateway. Secondly, it is possible to observe that Orange Pi and Raspberry Pi had acceptable results generating AES keys and appending new information in the IoT ledger. And, finally, some results about recurrent updates on block's ledger were presented. As can be observed in Figure 3 and Figure 4, it was possible to append information to the IoT ledger without compromising the communication with the device.

Although the proposed IoT ledger-based architecture presented good results, some aspects were not addressed in this work. First, it was considered, as a premise, that every device's public key was previously registered in the IoT ledger. Also, the impact of the consensus algorithms on the IoT ledger was not discussed. Moreover, the scalability of the proposed solution was not evaluated. These aspects are being assessed and they will be discussed in a future work.

V. Final Considerations

We have proposed a distributed access control solution for IoT. In order to manage the access control, we proposed the adoption of an IoT ledger-based architecture, in which gateways play an important role to manage access to devices information and controlling their communication. Thus, blockchain usage is a promising way to keep devices information updated over IoT gateways. Also, as the IoT ledger maintains the public key of each device, devices access could be managed by any gateway in the IoT network.

During the experimental evaluation we analyzed different hardware performance on cryptography algorithms. Based on the evaluation presented in this paper, Raspberry Pi 2 and Orange Pi Zero can be used as gateways in the IoT architecture proposal, and Arduino, due to its power processing limitation, could run as device in an edge to manage sensors and actuators. Moreover, the proposed IoT ledger-based architecture was evaluated into a scenario based on real office composed by gateways and devices. In this evaluation, the performance to handle data from devices presented good results, taking less than 0.07 seconds to append new information.

The proposed IoT ledger-based architecture is a promising solution to help in IoT access control. As presented in the experimental evaluation, devices and gateways with different hardware limitations could be used in the infrastructure with acceptable results. Finally, helping to answer the questions presented in the Introduction, (*i*) we presented that IoT devices can handle SHA256 and AES algorithms to communicate with IoT Gateways and RSA could be used for key exchange procedure; (*ii*) we proposed a solution that uses an IoT ledger to support Access Management in IoT networks; and, (*iii*) we evaluated the performance of different limited hardware sending encrypted data and updating an IoT ledger.

As future work, we intend to: *i*) evaluate different consensus algorithms to append new blocks from devices into the IoT ledger considering a larger scale scenario; *ii*) improve our solution to support different blockchain implementations, such as HyperLedger; and, *iii*) discuss how the data from devices could be stored in a cloud environment to reduce overhead on limited gateways.

Acknowledgment

This paper was achieved in cooperation with HP Brasil using incentives of Brazilian Informatics Law (Law n 8.2.48 of 1991). We also thank CAPES and SICREDI for the financial support. Finally, we thank Barbara Kudiess, Jonas Ayres and Suelen Strack.

REFERENCES

[1] J. A. Jerkins, "Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code," in *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, Jan 2017, pp. 1–5.

[2] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787 – 2805, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128610001568

[3] S. Cirani, L. Davoli, G. Ferrari, R. Lone, P. Medagliani, M. Picone, and L. Veltri, "A Scalable and Self-Configuring Architecture for Service Discovery in the Internet of Things," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 508–521, Oct 2014.

[4] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146 – 164, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128614003971

[5] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Www.Bitcoin.Org*, p. 9, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[6] F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 2084–2123, thirdquarter 2016.

[7] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schönwälder, "Using the RPL protocol for supporting passive monitoring in the Internet of Things," in *NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium*, April 2016, pp. 366–374.

[8] M. Tortonesi, J. Michaelis, N. Suri, and M. Baker, "Software-defined and value-based information processing and dissemination in IoT applications," in *NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium*, April 2016, pp. 789–793.

[9] A. Ouaddah, H. Mousannif, A. Abou Elkalam, and A. Ait Ouahman, "Access control in the Internet of Things: Big challenges and new opportunities," *Computer Networks*, vol. 112, pp. 237–262, 2017. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2016.11.007

[10] M. Abomhara and G. M. Kien, "Security and privacy in the Internet of Things: Current status and open issues," in *2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)*, May 2014, pp. 1–8.

[11] M. Conoscenti, A. Vetr, and J. C. D. Martin, "Peer to peer for privacy and decentralization in the internet of things," in *2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C)*, May 2017, pp. 288–290.

[12] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[13] S. Huh, S. Cho, and S. Kim, "Managing iot devices using blockchain platform," in *2017 19th International Conference on Advanced Communication Technology (ICACT)*, Feb 2017, pp. 464–467.

[14] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an Optimized BlockChain for IoT," in *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*, ser. IoTDI '17. New York, NY, USA: ACM, 2017, pp. 173–178. [Online]. Available: http://doi.acm.org/10.1145/3054977.3055003

[15] A. Boudguiga, N. Bouzerna, L. Granboulan, A. Olivereau, F. Quesnel, A. Roger, and R. Sirdey, "Towards better availability and accountability for iot updates by means of a blockchain," in *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, April 2017, pp. 50–58.

[16] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (iot) security: Current status, challenges and prospective measures," in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, Dec 2015, pp. 336–341.

[17] H. Ma, L. Liu, A. Zhou, and D. Zhao, "On networking of internet of things: Explorations and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 4, pp. 441–452, Aug 2016.

[18] M. M. Ahemd, M. A. Shah, and A. Wahid, "Iot security: A layered approach for attacks defenses," in *2017 International Conference on Communication Technologies (ComTech)*, April 2017, pp. 104–110.

[19] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: perspectives and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2481–2501, Nov 2014. [Online]. Available: https://doi.org/10.1007/s11276-014-0761-7

[20] H. Al-Mohannadi, Q. Mirza, A. Namanya, I. Awan, A. Cullen, and J. Disso, "Cyber-attack modeling analysis techniques: An overview," in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, Aug 2016, pp. 69–76.

[21] M. Conoscenti, A. Vetro, and J. C. D. Martin, "Blockchain for the internet of things: A systematic literature review," *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, pp. 1–6, 2016.